International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 1 Issue 9, November- 2012

To Identify and Eliminate Malicious Nodes in Cooperative Wireless Networks

R. Gopal, V. Parthasarathy and I. Infant Raj

ABSTRACT: *In a cooperative wireless network all the nodes will cooperate for the transmission of all other nodes. But there may be some malicious nodes which does not comply with the cooperation rule and act as selfish to reserve its resources for its own use. In this paper we present a review of the various approaches that are used to detect and eliminate the malicious nodes. We concentrated our review mainly on approaches that gave good results and which have to be improved. We provided our simulation result using NS2 with some routing protocols.*

Keywords: Cooperative - Malicious – Wireless - Technique, Reputation - Ns2 - Consensus - CoopMAC - Confidant.

1. INTRODUCTION

Cooperation among devices in a wireless network is more important as it leads to more efficient use of the network itself. Cooperation in the sense that if a node A wants to send a data to another node, the intermediate node helps the sender node in sending the packet to the destination properly. So from the above, we can say that the co-operator node may work in two ways. Such as 1) it may be the intermediate node which receive data from the source and 2) it may be the intermediate node which forwards the packet to the destination.

In both the cases, the co-operator node must use its own resource to receive or to forward the packet from source or to the destination. As these resources are not used for its own transmission, the devices or nodes begins to act as selfish or malicious node in the network to reserve its resource for its own transmission. In particular they try to reserve their bandwidth and batter power as they are the most limited resources. So this type of selfish node will not forward the packets that are assigned to them for forwarding thus it reserves its resources. Due to the packet drop by the selfish or malicious nodes, the total network performance will get degraded.

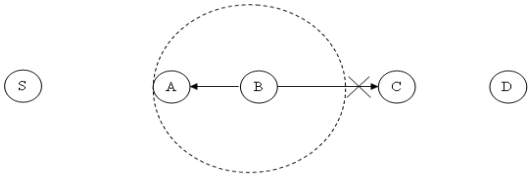

Fig.1 FA – Malicious Nodes as Honest

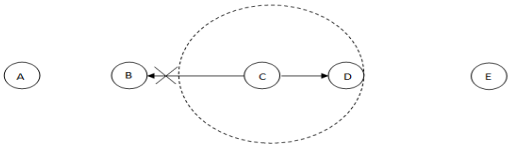

Fig. 2 FA – Honest Node as Malicious

In fig.1 node A and B are nearer to each other and node C is away from node B than node A. Node A send the data packet to node B, Node B acts as malicious nodes i.e., it does not send the data packet to node C but it send the acknowledgement to node A to save its energy resources. So node B acts as malicious but understood as honest node. In fig.2 node B is far away from node C than node D to node C. node B send data to node C. node C in turn sends the data packet to node D and sends the acknowledgement to node B with the same power used to send data to node D to save its energy.

So many techniques have been proposed by notable researchers to improve the cooperation of devices in a network by detecting and eliminating the selfish or malicious nodes from the network which in turn improves the performance of the network.

This paper is organized in as follows: in section 2, we discuss the Reputation Based Systems that are based on the Bayesian network proposed by Josang et al. In section 3, we discuss CoopMAC Protocol with ARQ proposed by Sintaehu Dehine et al. In section 4, we discuss CONFIDANT proposed by Buchegger et al. In section 5, we discuss Consensus Based Algorithm for detection of malicious nodes proposed by Stefano Tomasin et al. in section 6, we shown our simulation results. Finally in section 7, concludes the paper.

2. REPUTATION BASED TECHNIQUE

Josang et al propose a Bayesian network [4, 12] in which there will be a single central authority maintains and updates the reputation values of all the other nodes in the network. The central authority calculates the reputation values based on two variables. They are the total number of positive feedback and the total number of negative feedback for that node. Other nodes can get this information upon request. To make reputation calculation dynamic, the central authority decays both positive and negative ratings as a function of time. The central authority weights the creditability of the agent which provides the reputation value of a node to it. The new value will be added to the existing reputation value to form an updated reputation value.

There are various disadvantages in this approach as follows:

- The approach cannot be used in the distributed applications as it considers the central authority for reputation calculating.
- The use of decay function in reputation calculation is not sufficient approach to update the reputation value.
- In this approach the future reputation value cannot

be predicted.

- There is no any pictorial representation for the reputation relationships between the nodes.
- The model for reputation is not context specific.

2.1 Punishment Based Technique:

It is one of the reputation based system in which there are four steps followed to identify the malicious nodes and remove them from the network. The first step is identifying the misbehaving nodes such as selfish or malicious nodes. In the second step, the trust manager sends alarm about the malicious nodes. In the third step, the reputation system will assign values to the nodes based on the observations made by it and by others. In the last step, the path rather rates the path based on the values given by the reputation system and detect the path in which the malicious node present and act according to the routing request.

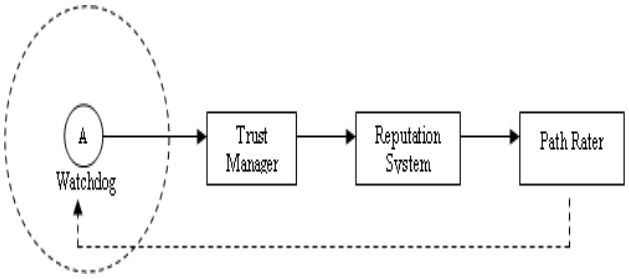

Fig. 3 Punishment Based Technique

2.2 Watch Dog Technique

Promiscuous Mode monitoring approach (Watchdog) [7] is one of such technique which is used to identify the malicious node. It is implemented with a routing protocol and relies on monitoring the neighbours. Each node in the transmission path monitors its successor node by overhearing the channel. Monitoring node will find the monitored node as malicious node if it drops the packets more than the threshold value. But it suffers from power control technique [11]. In fig. 3 the nodes A sends data to node B, in turn node B send data to node C and receive an acknowledgement from it. Now node A watch node B for acknowledgement from it for successful transmission.

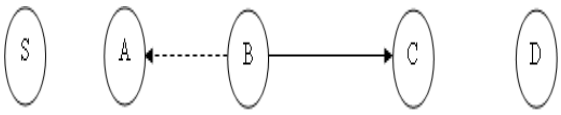

Fig. 4 Watch Dog

2.3 Two – Hop Ack Technique

Two-hop ACK [7, 10] is a technique in which the Acknowledgement travels two hops. By using this node can monitor its successor by receiving the Two-Hop ACK. In fig. 4, node A send data to node B which in turn forward the data to node C. node A now decide whether the node B malicious node or not by the acknowledgement received from node C to itself. If it receives the acknowledgement from node C then the node B is honest otherwise not.

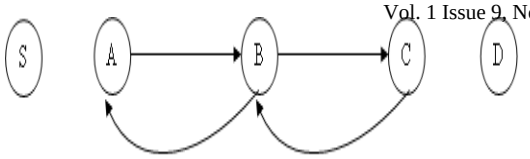

Fig. 5 Two – Hop Ack

2.4 Incentive and Eigen Trust Technique

Incentive technique [2] is one in which the node will be charged for its own transmission and reimbursed when it help for the transmission of other nodes. In this method for incentive purposes we use virtual currency also called as nuggets and the other one is priority for bandwidth. The nuggets are of two types' packet purse model and packet trade model. In packet purse model, the sender will add some nuggets in the packets which can be taken by any node that forward its packet. In packet market model, every node will purchase the packet from its previous node by using some nuggets and sell it to the next node for some nuggets.

Likewise Eigen Trust [3] is a technique based on the reputation, in which nodes ask all other nodes about the behaviour of all the nodes. Based on reputation the detection is done.

3. COOPMAC WITH ARQ

CoopMAC Protocol [2] has its implementation in the MAC layer of a wireless network. In this approach we use the CoopMAC and Automatic Repeat Request (ARQ) protocols. These two approaches are based on the Uniformly Most Powerful (UMP) and the Sequential Probability Ratio Test (SPRT). CoopMAC Protocol works as follows. Let us consider that node s wants to have cooperation transmission to node D through node C. The node S first sends a special Request to Send (RTS) packet which contains the requested rate in the link S-C and in the link C-D. Now node D sends a Clear – to – send (CTS) packet to node S and node C sends a Helper ready to send (HTS) packet to node S. On receiving both the CTS and HTS packets node S, starts the transmission. The reception of data by node C and D are acknowledged to node S through an acknowledgement (ACK). A node in CoopMAC Protocol can behave in two cases: it can be the destination or it can be the cooperating node in transmission between some other nodes. Here the Distributed Misbehaviour Detection Technique is used in which all nodes detect the misbehaving nodes by monitoring the control packets. In centralized approach, the same technique can be applied in where patrolling nodes decodes the control packets and detect malicious activity of the nodes and spread this to all other nodes. A false alarm happens when a honest node is taken as malicious node and a miss detection happens when a malicious node is taken as a honest node.

With ARQ, the node that transmits the data keeps re-transmitting the same coded data packet at each frame. The receiving node does not store the past versions of the same coded data packets. So it's assumed that the malicious node will use the same strategy to all the frames. The UMP will have large number of observations to find out the malicious nodes whereas SPRT needs a minimum number of observations to detect the malicious nodes. SPRT has minimum complexity than UMP. HARQ protocol used to

detect malicious nodes must perform multiple tests. i.e., test for each and every HARQ frame.
The shortcomings in this approach are as follows:

- In this approach, there is traffic overhead in the network by passing the control packets.
- The Expected Detection Delay is higher.
- It has to maintain a coop table, which contains the information about all the helper nodes.

4. CONFIDANT

Buchegger et al proposed an approach [3] in which the trust based decisions are made and the nodes with high trust value will be selected for the transmission of the data. The node with high trust value will not drop the packets. In order to assign the trust value for a node, the node will use its own interactions with that node and based on the response it mark the behaviour of the given node as satisfactory or unsatisfactory. These values will be updated based on the future interactions with the same node. But in the updating process, less weight will be given to the previous behaviour and more weights are given to the new behaviour. In addition to this is also it ask recommendation from other nodes also. So the final updated value will be shared with other nodes in the network. The trust values are calculated from the prior probabilities by using the bayes rule.

There are various disadvantages in this approach and those are as follows:

- It cannot differentiate between the loss due to bad channel condition or due to malicious activities.
- The model for reputation does not take into account its context specific nature.
- The future reputation value cannot be predicted.
- The use of decay function in reputation calculation is not sufficient approach to update the reputation value.
- The reputation relationships are not showed as pictorial representation for ease of comprehension and ease of representation.

5. CONSENSUS BASED ALGORITHMS

Stefano Tomasin proposed a technique [1] used to detect and eliminate the malicious nodes in the wireless network. In this technique, the CUSUM is used to detect the malicious nodes and the SPRT block, is used to find whether the CUSUM result is a False Alarm or the activity made by the malicious nodes.

The next step is to merge all these local opinions to form global opinions in the Fusion Centre. The possibility of the false alarm is considered while creating the global opinions. The global opinions are formed by using the maximum cardinality approach. There might be a situation in which the node n acts as malicious with some nodes and honest to all other nodes. At regular intervals, each node computes the value of $e_{m,n}$ and forwards this value to the Fusion Centre. If the value of $e_{m,n}$ is one then it is a honest node. Otherwise it is zero. So the Fusion Centre finds the honest nodes and takes necessary action against the malicious nodes.

The honest node list are formed by using

$$\mathcal{H}_{\mathrm{MC}} = \mathrm{argmax}_{\mathcal{H}\in\mathcal{C}}||\mathcal{H}||,$$

Where all set satisfy the property: $\forall n, m \in \mathcal{H}$, $e_{m,n}=1$.

We use the iterative approximate algorithms to determine $\mathcal{H}_{\mathrm{MC}}$. We build the set $\mathcal{H}_{\mathrm{MC}}$, which contain all the nodes and by iteratively we start removing the nodes that are not fully trusted. This step will be followed until all the nodes in the set are trusted by all other nodes in the set. The node that has the minimum number of good opinions will be removed. By removing the node c(j) from g(j) we increase the number of good opinions in the set g(j).
There are various shortcomings in this approach and they are as follows:

- The team activity of the malicious node is not considered in this technique.
- The expected detection delay is high.
- The optimal maximum clique search needs more operations to identify the malicious nodes.

6. SIMULATION RESULT

We simulated and studied the packet delivery ratio in presence of malicious node by using the routing protocols such as AODV, DSR, std AODV, std DSR in NS2. Our simulation environment consists of 500 wireless nodes in an area of 500 meter. We run the simulation for N number of times and the average of all these simulations are taken and a graph has been plotted. From the graph it is see that the AODV is better than DSR Protocol. At sometimes it seems that the packet delivery ratio is higher when there is more number of malicious nodes. This is due to the reason that only the path without malicious nodes are taken for data transmission.

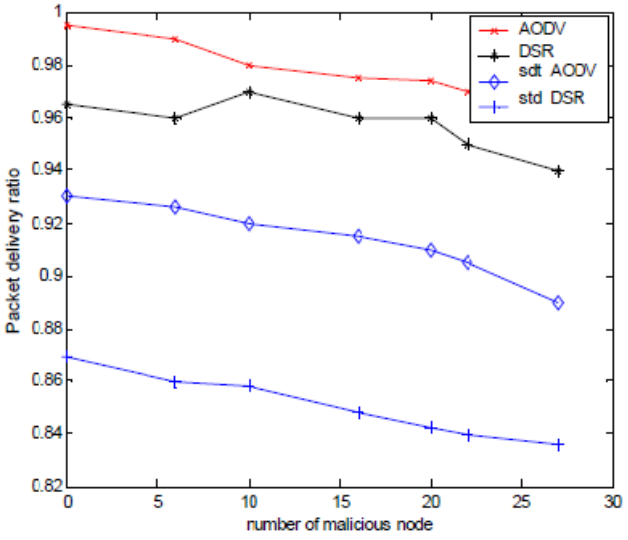

Fig. 6 Packet Delivery Ratio

7. CONCLUSION

In this paper we presented an overview of the techniques that are used to detect and eliminate the malicious nodes in a cooperative wireless network. We hereby like to propose a technique to detect and eliminate the malicious nodes from the network which increase the

performance of the entire network. Here the team activity of the malicious node is considered and the expected detection delay is made minimal. Malicious nodes are detected with minimum operations which in turn reduce the time to detect them.

REFERENCES

[1] Stefano Tomasin, "Consensus-Based Detection of Malicious Nodes in Cooperative Wireless Networks," IEEE COMMUNICATIONS LETTERS, VOL. 15, no. 4, April 2011
[2] S. Dehnie and S. Tomasin, "Detection of selfish nodes in networks using CoopMAC protocol with ARQ," *IEEE Trans. Wireless Commun.*, vol. 9, no. 7, pp. 2328–2337, July 2010.
[3] S. Buchegger and J.-Y. Le Boudec, "Performance analysis of the confidant protocol: cooperation of nodes–fairness in distributed ad hoc networks," in *Proc. 3rd ACM Int. Symp. on Mobile Ad hoc Netw. And Computing*, 2002, pp. 226–236.

[4] F. K. Hussain, E. Chang, and O. K. Hussain, "State of the art review of the existing Bayesian-network based approaches to trust and reputation computation," in *Proc. 2nd Int. Conf. on Internet Monitoring and Protection*, July 2007.
[5] N. Shastry and R. S. Adve, "Stimulating cooperative diversity in wireless ad hoc networks through pricing," in *Proc. IEEE Int. Conf. Commun.(ICC)*, vol. 8, June 2006, pp. 3747–3752.
[6] S. D. Kamvar, M. T. Schlosser, and H. Garcia-Molina, "The Eigen trust algorithm for reputation management in p2p netowkrs," in *ACM International Conference on World Wide Web*, 2003, pp. 640–651.
[7] D. Djenouri and N. Badache, "Struggling against selfishness and black hole attacks in MANETs," *Wireless Commun. and Mobile Computing*, no. 8, pp. 689–704, 2008.
[8] M. Kim, R. Kotter, M. Medard, and J. Barros, "An algebraic watchdog for wireless network coding," in *Proc. Int. Symp. Info. Theory*, pp. 1159–1163, June 2009.
[9] J. M. Robson, "Algorithms for maximum independent sets," *J. Algorithms*, vol. 7, no. 3, pp. 425–440, 1986.
[10] D. Djenouri and N. Badache, "A novel approach for selfish nodes detection in manets: Proposal and petri nets based modeling," in *The 8th IEEE International Conference on Telecommunications (ConTel'05)*, Zagreb, Croatia, June 2005, pp. 569–574.
[11] D. Djenouri and N. Badache, "New power-aware routing for mobile ad hoc networks," *The International Journal of Ad Hoc and Ubiquitous Computing (Inderscience Publisher)*, vol. 1, no. 3, pp. 126–136, 2006.
[12] Audun Jøsang and Roslan Ismail, "The Beta Reputation System", Proceedings of the 15th Bled Conference on Electronic Commerce, Bled, Slovenia, 17-19 June 2002.

Authors Biography

Author 1 has completed his B.E and M.E in Computer Science and Engineering from PGP college of Engineering and Technology, Namakkal, and Mahendra Engineering College, Tiruchengode respectively in 2005 and 2010.He currently is pursuing Ph.D. from Chettinad College of Engineering and Technology under Anna University-Chennai. He has six years of teaching and research experience in Chettinad College of Engineering and Technology, Karur and currently he holds the post of Assistant professor in the Department of Computer Science and Engineering, Chettinad College of Engineering and Technology, Karur, Tamilnadu, India. His email id is rgopalkarur@gmail.com

Author 2 has completed his B.E and M.E in Electrical and Electronics Engineering from Government College of Technology, Coimbatore and M.E in Computer Science and Engineering in College of Engineering Anna University, Chennai in 2004. He then completed his Ph.D. from Anna University-Chennai in 2010. He has seventeen years of teaching and research experience in Chettinad college of Engineering and Technology and currently he holds the post of Principal in Chettinad college of Engineering and Technology, Karur, Tamilnadu, India. He has published more than 31 research papers in various conferences and journals. His email id is sarathy.vp@gmail.com

Author 3 has completed his B.E in Computer Science and Engineering from RVS College of Engineering and Technology, Dindigul. He currently is doing M.E in Chettinad College of Engineering and Technology under Anna University-Chennai. 2011 and 2013.His email id is infantirudayam@gmail.com.